NASA Procedures and Guidelines

NPG: 2810.1

Effective Date: August 26, 1999
Expiration Date: August 26, 2004

SECURITY INFORMATION TECHNOLOGY

Responsible Office: AO/Chief Information Officer

Excerpt from NPG 2810.1

4.8. Appropriate Use of Information Technology Resources

4.8.1. Overview

4.8.1.1. The following guidance is provided for the appropriate, ethical, and legal use of IT resources belonging to NASA. This section answers commonly asked questions about these topics and to give managers at all levels a common baseline for discussing these topics with their employees.

4.8.1.2. Laws concerning computers and computer crimes are constantly changing. To get the most recent information about laws related to computer crimes, consult the Center's Office of Chief Counsel. To get the most recent information about computer usage policy matters, contact the Human Resources Office, CIO, or Center IT Security Manager.

4.8.2. Official Business Use of Government Resources

NASA provides computer systems for the purpose of transacting official business. The following sections provide guidance on what is considered official business use, what is not considered official business use, and what use may be considered acceptable use with proper approval.

4.8.3. Official Business Uses

4.8.3.1. Official business broadly includes any computer processing that is required as part of the job. Official business includes, but is not limited to, the performance of NASA work-related duties in position descriptions, professional training and class work, work covered under grant agreements with NASA, tasks directed via NASA contracts, agreements with international partners, Center-authorized activities, and support activities related to NASA contract tasking.

4.8.3.2. With the concurrence of appropriate Center management, some less formal activities may be authorized. Authorization for such activities should be documented by management and may include, but not be limited to, the following:

a. Work-related events, such as a technical symposiums, classes, and presentations.

b. Activities sponsored by the Center, such as child care center and carpooling activities.

c. Events and activities specific to a particular NASA or Center organization.

d. Center-sanctioned activities, such as blood drives, sanctioned clubs, and organizations.

4.8.3.3. Management may permit some infrequent personal use of electronic mail. When communication cannot reasonably be made during non-business hours, employees may exchange brief messages with such persons or entities as the following:

a. Spouse or dependent.

b. Someone responsible for the care of a spouse or dependent.

c. State and local government agencies on personal matters.

d. Medical care providers.

e. Dentists.

f. Users may also use electronic mail in emergency situations.

4.8.4. Other Permissible Uses

4.8.4.1. Because there is no measurable cost, some limited personal use of Internet services, such as the World Wide Web and electronic mail, is permitted, provided it does not interfere with the employee’s work or the work of others. Extreme care must be taken regarding content matter. Under no circumstances is it permissible to access or download material that would create a hostile or offensive work environment, such as racist or sexually explicit material. Use must be kept to brief periods when it can reasonably be assumed that the employee is in a nonduty status, such as during lunch breaks.

4.8.4.2. Some uses of NASA computer systems are clearly outside the boundaries of official business and permissible use. Prohibited uses of NASA’s IT resources include using systems to do the following:

a. Maintaining or conducting an outside business.

b. Monitoring network traffic (e.g., run a sniffer); access IT resources; or copy data, files, or software without prior authorization. (Activities for which prior authorization is assumed include performing defined job duties, copying information that is intended to be copied, and doing work that has been approved by the Center IT Security Manager.)

c. Participating in Chat Rooms, News Groups, or similar activities where the posting will be seen by the public. Use of the NASA Internet address of "nasa.gov" is a representation of the Agency, analogous to the use of NASA letterhead in which the opinions expressed reflect on NASA.

d. Advertising goods or services for sale for monetary or personal gain.

e. Sending chain letters, personal mass mailings, hoaxes, or harassing messages.

4.8.4.3 Users should be particularly careful about using NASA computer systems in any way that could be interpreted as intending to influence any member of Congress to favor or oppose any legislation or appropriation. If the offender is an officer or employee of the United States, such an act may fall under a provision of Title 18 U. S. Code, Section 1913, "Lobbying with appropriated monies," which carries severe penalties upon conviction. If there are any questions about any aspect of this provision of law, contact your Center's Office of Chief Counsel for advice and assistance.

4.9. Software Usage

4.9.1. Overview

All users of NASA resources must comply with the terms of any license agreement for any software that NASA provides. It is usually illegal in the United States and most other countries to make or distribute copies of copyrighted material without authorization from the copyright holder. The NASA OIG, line managers, and other authorized individuals occasionally audit U.S. Government-owned equipment for the presence of unlicensed software. Each user is responsible for reading and complying with the terms of the license agreement that accompanies software.

4.9.2. Usage Guidelines by Software Type

The following are guidelines for appropriately using software:

a. Public Domain Software--Some software authors choose to make their software publicly available under terms that the author may specify. This public domain software may be used on NASA computers at the option of the line manager.

b. Shareware--Shareware is software that is available for a trial period at no cost. Users who wish to continue using shareware after the trial period may then be required to pay a license fee. Shareware is permitted on NASA computers at the option of the line manager, but the license fee must be paid.

c.   Software Use at Home--Many users have workstations at home where they perform job-related work. Some software licenses accommodate use at home as well as at work. Some licenses may even permit personal home use of Government-purchased software. NASA allows users to make any legitimate use of a Government-purchased software package that is consistent with the license agreement. The burden is on the user to understand and to comply with that agreement.

d.   Inspection of Imported Software for Malicious Code--All software entering the NASA community is called "imported software." Before being installed on any NASA-owned computer, all imported software must be approved by the responsible line manager. Each line manager may have a slightly different approval process, but all approval processes must include a check for the presence of malicious code, such as viruses, trap doors, and trojan code. Diskettes that users bring from home and diskettes that they bring back from travel have in the past been fertile sources of computer viruses. The use of imported software is permitted, but the user must take responsibility for examining it for the presence of malicious code before installing it. NASA and its immediate contractor community are required to have a process in place to inspect imported software. For more assistance, contact your organizational CSO.

4.10.   Access Warning Banner, Notification of Rights, and Monitoring

4.10.1. Overview

Government computer systems may be targets of hostile activities and subject to other forms of unauthorized use. To counter these activities, the Government may monitor and record the use of Government computer systems through keystroke monitoring and other methods. To deter misuse and notify all users that their use may be monitored, guidance is provided on implementing a warning banner on all appropriate NASA computer systems. This direction applies to all NASA-owned or NASA-funded IT systems, regardless of location or user, including Government-provided equipment.

4.10.2. Notification to Users at Logon

4.10.2.1. A NASA standard banner shall be loaded onto all computer systems covered by this guidance so that it is affirmatively displayed at the time a user boots his or her system or is initially challenged for an authentication. Users without a "nasa.gov" domain address will see the NASA standard banner only when the NASA system they are attempting to access requires a user password identification.

4.10.2.2. Since new laws regarding employee expectations of privacy on employer IT resources are being tested in the courts and old laws are being applied in cases involving IT, consult the Center IT Security Manager for the latest NASA standard banner.

4.10.2.3. The NASA standard banner is intended as a minimal warning to effect the objectives described in the overview, above. In cases where there are reasons to deviate from, supplement, or not implement the standard banner, such exceptions shall be approved by the Center CIO or designee and concurred in writing by the servicing Chief Counsel (in the case of Headquarters, Office of the General Counsel) and local Inspector General. Line managers should work through their assigned legal counsel to seek the advice and concurrence of their local Inspector General. The Center IT Security Manager shall maintain documentation for approved exceptions.

4.10.3. Notification of Rights to IT Resources

4.10.3.1. All NASA computer systems, like all systems that belong to the U. S. Government, are subject to audits. Users should realize that they do not have any expectation of privacy when they use a NASA computer system.

4.10.3.2. Every user of a NASA-owned computer system should understand that the computer equipment, software, and information they contain are not their property. They are the property of the U.S. Government, a cooperating foreign government, corporate entity, research center, university, or other entity as specified in the agreement or contract that originally permitted access to the system.

4.10.4. Monitoring of IT Resources

4.10.4.1. All activities on NASA's computer systems may be monitored to the extent permitted by law and NASA directives. This monitoring may include traffic analysis, keystroke monitoring, examination of log files, and examination of any or all files on the computer. Monitoring may be initiated any time evidence of apparent misuse or possible criminal activity has been reported.

4.10.4.2. All files in a user's account, including electronic mail, may be examined under appropriate circumstances by the following staff:

a. Line manager.

b. Officials representing the Center CIO.

c. Director of Human Resources.

d. Office of Chief Counsel.

e. Representatives from the CCS.

f. Representatives of the OIG.

g. Other law enforcement officials.

4.10.5. Notice of Information Gathering

If a system (e.g., WEB pages or News Groups) is gathering information on an individual's identity or activities, the system must provide a warning, notifying the individual what information is being collected and what will be done with the information. Gathering statistical data (e.g., usage, domains, traffic loading) not identified with an individual is permitted. For guidance see the Center IT Security Manager.